Document RFC 2350

GOV CERT SK

1. Document Information

1.1 Date of Last Update

This is version 1.0 as of 31st January 2017.

1.2 Distribution List for Notifications

Concerning RFC 2350 changes there is no distribution list for notifications provided by GOV CERT SK.

1.3 Locations Where this Document May Be Found

The current version of this document is available at website – **www.cert.gov.sk**

2. Contact Information

2.1 Name of the Team

GOV CERT SK

2.2 Address

Národná agentúra pre sieťové a elektronické služby
GOV CERT SK
BC Omnipolis
Trnavská cesta 100/II
821 01 BRATISLAVA

2.3 Time Zone

CET, Central European Time (UTC+1, from the last Sunday in October to the last Saturday in March)
CEST, Central European Summer Time (UTC+2, from the last Sunday in March to the last Saturday in October)

2.4 Telephone Number

+421 2 3278 0700

+421 2 3278 0780

2.5 Facsimile Number

Not available

2.6 Other Telecommunication

Not available

2.7 Electronic Mail Address

For the incident reports, please use the address **incident@cert.gov.sk**

Non-incident related mail should be addressed to **info@cert.gov.sk**

2.8 Public keys and encryption information

For the incident related communication, you can use this key:

GOV CERT SK (NASES)

PGP Key ID: 0xCA4685063EC53992

PGP Key Fingerprint: 5E9B 77EC AE23 530B 56C5 2CB7 CA46 8506 3EC5 3992

The key is available for download in the TXT format here **ASC**

2.9 Team members

Information about GOV CERT SK members is not published.

Management and control is provided by the Director of the Security Division of the National Agency for Network and Electronic Services.

2.10 Other Information

More information about GOV CERT SK is available at **www.cert.gov.sk**

2.11 Points of Customer Contact

The preferred method to contact GOV CERT SK is an e-mail.

For general inquiries and questions please send e-mail to **info@cert.gov.sk**

For incident reports and related issues please use **incident@cert.gov.sk**

In urgent cases, please put URGENT in the subject of the report.

If it is not possible (or due to security reasons) to use e-mail, you can reach GOV CERT SK via telephone at +421 2 32 780 780 during workin hours from 08:00 to 18:00 hod. from Monday to Friday, GMT +01:00, except national holidays.

3. Charter

3.1 Mission Statement

GOV CERT SK carries out activities in the field of GOVNET network security, central information infrastructure and central communication infrastructure for public administration of the Slovak republic.

3.2 Constituency

In the constituency of GOV CERT SK are public administration bodies and solving of security incidents at the national level, as well as continuous monitoring of government network Govnet, Central Government Portal and other operated projects and information systems of NASES.

3.3 Sponsorship and/or affiliation

GOV CERT SK is an affiliate branch of the National Agency for Network and Electronic Services.

3.4 Authority

GOV CERT SK operates in accordance with the statues of the National Agency for Network and Electronic Services.

GOV CERT SK cooperates with system administrators and operators of public sector institutions.

4. Policies

4.1 Types of Incidents and Level of Support

GOV CERT SK is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency. The level of support given by GOV CERT SK will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the GOV CERT SK´s resources at the time.

No direct support will be given to end-users.

GOV CERT SK will provide cooperation as soon as possible.

Within its sphere of competence the GOV CERT SK will provide support to administrators of information systems of public administration networks.

GOV CERT SK is committed to keep the constituency informed of potential vulnerabilities, and where possible, will inform theirs of such threats and vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by GOV CERT SK, regardless of its priority. Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

GOV CERT SK will use the information you provide to help solve security incidents. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymous fashion.

GOV CERT SK operates within the bounds of the Slovak legislation.

4.3 Communication and Authentication

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident response

The goal of GOV CERT SK is to solve and to provide co-ordination of security incidents (defined in 3.2). Provides assistance or advice in the following aspects of incident management:

- alerts and warnings,
- incident response
- analysis of ongoing incidents,
- provide documentation to help handle certain common incidents,
- coordinating responses to incident handling,
  response and analysis of malicious software,
- Govnet point of contact.

5.2 Proactive activities

GOV CERT SK coordinates and provides:

- notifications of security warnings, consultancy and related information,
- security awareness-raising seminars and courses,
- coordinates preventive measures against cyber vulnerability,
- cooperates with competent authorities to identify security threats.

6. Incident reporting forms

There are no incident reporting forms available.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, GOV CERT SK assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.